**Eksamen 2. juni 2015** **IR201712 Diskret Matematikk**
**Eksamenstid 4 timar** *Nynorsk*

**Ingen hjelpemiddel er tillatne.**
Ta med **all mellomrekning** som trengst for å grunngje svaret.

Oppgåve 1 ..... *(4%)*

(a) Rekn ut $\binom{6}{4}$.

(b) Rekn ut $\binom{640}{639}$.

Oppgåve 2 ..... *(7%)*

Rekn ut fylgjande

(a) $(5+8) \mod 9 =$

(b) $(9 \cdot 6 + 3) \mod 19 =$

(c) $(x^2 + x + 1) \cdot (x + 1)$ over $\mathbb{Z}_2$.

Oppgåve 3 ..... *(5%)*

Løys fylgjande kongruensar (modulære likningar)

(a) $2x \equiv 1 \pmod 3$

(b) $3x + 2 \equiv 1 \pmod 5$

Oppgåve 4 ..... *(4%)*

(a) Skriv det heksadesimale talet 2C om på desimalform.

(b) Skriv talet 20 (desimal) på heksadesimal form.

Oppgåve 5 ..... *(12%)*

Me har eit datasystem med brukarnamn og passord. Forklar korleis me finn talet på unike, moglege passord, når

(a) ... passordet må bestå av nøyaktig seks små, norske bokstavar?

(b) ... passordet må bestå av seks til åtte små, norske bokstavar?

(c) ... passordet må bestå av seks til åtte teikn der *det fyrste* er ein stor norsk bokstav, og resten kan vera anten store eller små bokstavar?

Det er tilstrekkeleg å setja opp formlar og setja inn tal. Du **treng ikkje** å rekna ut formlane. Forklar kva teljeprinsipp du treng og korleis du kjem fram til formlane i kvart delspørsmål.

Oppgåve 6 ..... *(6%)*

I dette spørsmålet ser me på logiske argument.

(a) Sjå på dei to utsagna

1. Dersom det regnar, tek eg på regnjakke.
2. Det regnar.

Kva slutning kan du trekkja frå desse to premissane ved hjelp av direkte prov (Modus Ponens)?

(b) Sjå på argumentet

1. $s \Rightarrow t$
2. ??

$\therefore \neg s$

Kva utsagn må du setja for spørsmålsteikna for at argumentet skal vera gyldig (Modus Tollens)? (Symbolet $\therefore$ kan lesast som «ergo» eller som «dermed kan me konkludera med at».)

Oppgåve 7 ..... *(5%)*

Forklar kva me meiner med ein nulldivisor, og list opp nulldivisorane i $\mathbb{Z}_{12}$.

Oppgåve 8 ..... *(4%)*

Krypter meldinga «godmorgen» med Cæsars siffer. Vis fullstendig korleis meldinga kan krypterast ved å bruka modulær aritmetikk over heiltal.

Oppgåve 9 ..... *(8%)*

(a) Lat $A$ og $B$ vera matrisar over $\mathbb{Z}_2$:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Rekn ut $A \cdot B =$

(b) Lat $C$ og $D$ vera matrisar over $\mathbb{Z}_5$:

$$C = \begin{bmatrix} 1 & 2 \\ 0 & 3 \\ 0 & 4 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 4 \\ 3 & 2 \end{bmatrix}$$

Rekn ut $C \cdot D =$.

Oppgåve 10 ..... *(12%)*

Tenk på relasjonen $<$ (mindre enn)

(a) Kva meiner me (generelt) med ein relasjon?

Svar på fylgjande tre spørsmål om $<$-relasjonen og grunngje kvart svar:

(b) Er $<$ symmetrisk?

(c) Er $<$ refleksiv?

(d) Er $<$ transitiv?

Oppgåve 11 ..... *(12%)*

(a) Vis steg for steg korleis du bruker Euklids algoritme for å finna $\text{hcf}(413, 273)$[1]?

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 11 modulo 91.

(c) Gjeve $\text{hcf}(a, b)$, korleis veit me om $a$ hev ein multiplikativ invers modulo $b$?

Oppgåve 12 ..... *(16%)*

RSA har krypteringsfunksjonen $e_{e,n}(x) = x^e \mod n$.

(a) Vis, steg for steg, korleis du reknar ut $16^{14} \mod 21$ på ein effektiv måte.

(b) Skriv pseudo-kode for ein effektiv algoritme for å rekna ut $x^e \mod n$.

(c) Prov at algoritmen frå (b) avsluttar i endeleg tid.

(d) I krypteringsfunksjonen over er $(e, n)$ den offentlege nykkelen. Forklar korleis den løynde (private) nykkelen er definert eller korleis han vert rekna ut.

Oppgåve 13 ..... *(5%)*

Sjå på rekurrenslikninga

$$T(n) = 2 \cdot T(n-1) + 1,$$
$$T(0) = 1.$$

Bruk matematisk induksjon til å prova at $T(n) = 2^{n+1} - 1$ for alle $n \geq 0$.

[1] hcf står for *Highest Common Factor* eller største felles divisor (ogso kjend som gcd).